

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068*

MASTER OF MILITARY STUDIES

***TITLE: ETHICAL CONSIDERATIONS OF COMPUTER NETWORK ATTACK
IN INFORMATION WARFARE***

**SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES**

AUTHOR: CDR MAXIE Y. DAVIS, U.S. NAVY

AY 00-01

Mentor: Dr. Albert C. Pierce

Approved:_____

Date:_____

Mentor: Colonel James M. McCarl Jr. and Mr. Thomas A. Sileo

Approved:_____

Date:_____

| Report Documentation Page | | |
|--|--|--|
| Report Date 16 Jan 2001 | Report Type N/A | Dates Covered (from... to) - |
| Title and Subtitle Ethical Considerations of Computer Network Attack in Information Warfare | Contract Number | |
| | Grant Number | |
| | Program Element Number | |
| Author(s) | Project Number | |
| | Task Number | |
| | Work Unit Number | |
| Performing Organization Name(s) and Address(es) Joint Military Operations Department Navy War College 686 Cushing Road Newport, RI 02841-1207 | Performing Organization Report Number | |
| Sponsoring/Monitoring Agency Name(s) and Address(es) | Sponsor/Monitor's Acronym(s) | |
| | Sponsor/Monitor's Report Number(s) | |
| Distribution/Availability Statement Approved for public release, distribution unlimited | | |
| Supplementary Notes The original document contains color images. | | |
| Abstract Computer Network Attack (CNA), a form of offensive IO, offers the war fighter a powerful capability, but like nuclear weapons, also poses magnanimous ethical challenges in its use. International laws that govern war written with kinetic force as a backdrop may or may not offer a straightforward application to this non-kinetic force. Just War Theory offers a broader base for ethical considerations of CNA. | | |
| Subject Terms | | |
| Report Classification unclassified | Classification of this page unclassified | |
| Classification of Abstract unclassified | Limitation of Abstract UU | |
| Number of Pages 53 | | |

| REPORT DOCUMENTATION PAGE | | FORM APPROVED - - - OMB NO. 0704-0188 |
|--|-------------------------------|---|
| <small>public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters services, directorate for information operations and reports, 1215 Jefferson Davis highway, suite 1204, Arlington, VA 22202-4302, and to the office of management and budget, paperwork reduction project (0704-0188), Washington, dc 20503</small> | | |
| 1. AGENCY USE ONLY (LEAVE BLANK) | 2. REPORT DATE 16 JAN 2001 | 3. REPORT TYPE AND DATES COVERED STUDENT RESEARCH PAPER |
| 4. TITLE AND SUBTITLE ETHICAL CONSIDERATIONS OF COMPUTER NETWORK ATTACK IN INFORMATION WARFARE | | 5. FUNDING NUMBERS N/A |
| 6. AUTHOR(S) CDR Maxie Y. Davis, US Navy | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC COMMAND AND STAFF COLLEGE 2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068 | | 8. PERFORMING ORGANIZATION REPORT NUMBER NONE |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) SAME AS #7. | | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER: NONE |
| 11. SUPPLEMENTARY NOTES NONE | | |
| 12A. DISTRIBUTION/AVAILABILITY STATEMENT NO RESTRICTIONS | | 12B. DISTRIBUTION CODE N/A |
| abstract (maximum 200 words) Computer Network Attack (CNA), a form of offensive IO, offers the war fighter a powerful capability, but like nuclear weapons, also poses magnanimous ethical challenges in its use. International laws that govern war written with kinetic force as a backdrop may or may not offer a straightforward application to this non-kinetic force. Just War Theory offers a broader base for ethical considerations of CNA. | | |
| 13. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH) Computer Network Attack, Information Operations, Just War Theory, International Law, Ethics | | 15. NUMBER OF PAGES: |
| | | 16. PRICE CODE: N/A |

| | | | |
|---------------------------------------|---|---|----------------------------|
| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE: | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
| <i>UNCLASSIFIED</i> | <i>UNCLASSIFIED</i> | <i>UNCLASSIFIED</i> | |

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT. QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

| | |
|--|------|
| MMS Cover Sheet..... | i |
| DISCLAIMER..... | ii |
| TABLE OF CONTENTS..... | iii |
| LIST OF ILLUSTRATIONS..... | iv |
| LIST OF TABLES..... | v |
| PREFACE..... | vi |
| EXECUTIVE SUMMARY..... | viii |
| CHAPTER ONE: Introduction..... | 1 |
| CHAPTER TWO: CNA and DOD Posture..... | 6 |
| Policy Guidance..... | 6 |
| Planning..... | 7 |
| CNA and Potential Targets..... | 8 |
| Methods of CNA..... | 11 |
| CHAPTER THREE: CNA and International Law..... | 15 |
| CHAPTER FOUR: Just War Theory and CNA..... | 20 |
| Right Authority | 24 |
| Just Cause | 24 |
| Right Intentions | 25 |
| Last Resort | 26 |
| Reasonable Hope | 27 |
| Proportionality of Ends | 28 |
| The Aim of Peace..... | 29 |
| Noncombatant Protection | 30 |
| Proportionality of Means..... | 30 |
| Overall Assessment..... | 31 |
| CHAPTER FIVE: Conclusion and Recommendation..... | 33 |
| GLOSSARY..... | 37 |
| BIBLIOGRAPHY..... | 41 |

Illustrations

| | |
|---|----|
| Illustration 1. Law and Ethics Moderate Overlap..... | 4 |
| Illustration 2. Law and Ethics Considerable Overlap..... | 4 |
| Illustration 3. Law and Ethics No Overlap..... | 4 |
| Illustration 4. Examples of Information Operations Targets..... | 10 |

Tables

| | |
|---|----|
| Table 1. The Just War Tradition as a Source of Criteria for Ethical Judgment..... | 21 |
|---|----|

Preface

This Master of Military Science (MMS) paper is an analysis of the ethical dilemma for the United States' National Command Authorities (NCA) and the Department of Defense (DOD) posed by offensive and counteroffensive use of Computer Network Attack (CNA) in Information Warfare (IW). Most of the work done by the DOD in this area is classified and no classified sources were used or read in support of this paper. The examples of CNA discussed are strictly conjecture or actual CNA proposals that have been declassified.

As an information technology manager with a working knowledge of computer vulnerabilities, an examination of the moral implications of exploiting such vulnerabilities seemed a worthwhile endeavor, particularly in light of the U.S. emphasis on developing CNA capabilities. While I may understand the technology to some degree and have experience in defensive information operations (IO) in the form of information assurance, I have no experience in offensive IO. In addition, my personal knowledge of international law and the Just War Theory is limited to that which was obtained through the research for this paper and course work at the United States Marine Corps Command

and Staff College. I have, however, received a significant amount of assistance and guidance from: Dr. Albert C. Pierce, PhD in Political Science, Director for Center For The Study of Professional Military Ethics, U. S. Naval Academy; Colonel James M. McCarl Jr., Army Intelligence Officer and Deputy Director of United States Marine Corps Command and Staff College who served as an IO Plans Officer in Desert Storm; and Mr. Thomas A. Sileo, the Central Intelligence Agency (CIA) Chair at the Marine Corps University, who has exposure to proposed and actual CNA operations as a CIA employee; a member of the Joint Chief's Staff, Information Operations (J39) and this staff's legal advisors.

EXECUTIVE SUMMARY

Title: Ethical Considerations of Computer Network Attack in Information Warfare

Author: Commander Maxie Y. Davis, United States Navy

Thesis: Moral considerations above those that are codified in international law should guide the use of Computer Network Attack in Information Warfare.

Discussion: Department of Defense (DOD) Joint Vision 2020 establishes information superiority as the foundation for its goal of full spectrum dominance. To achieve information superiority, further development and study of the use of defensive and offensive information operations (IO) capabilities are imperative, specifically in the area of Computer Network Attack (CNA). CNA, a form of offensive IO, offers the war fighter a powerful capability, as well as a myriad of technical, legal and ethical challenges in its use. The technology to support CNA is quickly maturing, but the same is not true of the application of legal and moral guidelines. Military leaders and lawyers are faced with the dilemma of evaluating proposed CNA against a legal and moral backdrop developed for the use of kinetic force. This dilemma suggests a re-examination of the genesis of legitimate use of force, the Just War Theory.

Conclusion and Recommendation: Using the Just War Theory provides a common framework, which may serve to garner international consensus on the moral use of CNA.

Chapter 1

Introduction

Protection of information assets is a genuine concern for the U.S. military and the country as a whole because of the vulnerability of its computer networks. The U.S. national information infrastructure (NII) and the Defense Information Infrastructure (DII) are embedded and deeply integrated in the expanding global information infrastructure (GII). This configuration presents to any would-be adversary an avenue to exploit, disrupt, or destroy U.S. information assets. According to Richard Aldrich, the potential risks are many, including "the opportunity to disrupt military effectiveness and public safety, with the elements of surprise and anonymity."¹ Along with U.S. efforts in information assurance, developments in computer network attack (CNA) capabilities may provide additional defense against cyber attacks on U.S. information systems.

As a capability, CNA may also be critical to gaining information superiority on the battlefield. Information superiority, as per the Chairman of the Joint Chiefs of

¹ Richard W. Aldrich, *Cyberterrorism and Computer Crimes: Issues Surrounding The Establishment of an International Regime*, INSS Occasional Paper 32, *Information Warfare Series* (USAF Academy, CO: USAF Institute for National Security Studies, 2000), 5.

Staff (CJCS) Joint Vision 2020, is fundamental to the transformation of the operational forces of today to a joint force that is "dominant across the full spectrum of military operations - persuasive in peace, decisive in war, pre-eminent in any form of conflict."²

The Unified Command Plan for 1999 (UCP-99) designated the United States Space Command (USSPACECOM) as the lead for Computer Network Defense, effective 1 Oct 99, and for Computer Network Attack (CNA), effective 1 Oct 00. In May 2000, the USSPACECOM CNA Activation Task Force delivered to the Joint Chiefs of Staff (JCS) classified documents that set forth the general manner in which the United States Commander In Chief of Space Command (USCINCSpace) will execute his responsibilities in CNA. Anticipating an increase in interest in CNA by the media and the general public, DOD public affairs guidance released on 1 Nov 00 addressed intended uses and legal implications of CNA.

Within DOD, USPACECOM is designated as the military lead for defending DOD networks and in the context of the Law of Armed Conflict, with denying an adversary the ability to use computer networks to conduct military operations. Attacking an adversary's computer network could also be an element of defending our own computer networks from a major cyber attack against our own systems. CNA operations may also be used in other situations. For example, combating terrorist threats when directed by appropriate

² Chairman, Joint Chiefs of Staff, *Joint Vision 2020* (Washington DC: U.S. Government Printing Office, 2000), 8.

authorities. Integrating CNA into a broader military operation will help U.S. Armed Forces to prevail on future battlefields. In some cases computer network attack might also allow an operation to succeed with less loss of life and physical destruction. As with any military capability, the United States will employ CNA after careful policy and legal review, and any use of CNA will be consistent with U.S. international obligations and the Law of Armed Conflict.³

This statement, the guidance in Joint Doctrine for Information Operations (Joint Pub 3-13), and the intimate involvement of the Judge Advocate General Corps in IO planning, speak to DOD's commitment to the legal use of CNA.

The focus of this paper is to support an expansion of the ethical considerations that the law dictates. Law and ethics are not the same and as such "it is a misconception to think of the international law of war as it has developed down to our time as containing all that there is to say about the justification and limitation of war."⁴

Dr. Albert C. Pierce, United States Naval Academy, uses Venn diagrams to show the relationship between law and ethics. Law and ethics can overlap a little (Illustration

³ SECDEF WASHINGTON DC//OASD-PA/DPL// Public Affairs Guidance – Computer Network Attack DTG 012050Z Nov 00.

⁴ James Turner Johnson, *Can Modern War Be Just?* (New Haven and London: Yale University Press, 1984), 15.

1), a lot (Illustration 2) or sometimes not as all (Illustration 3):⁵

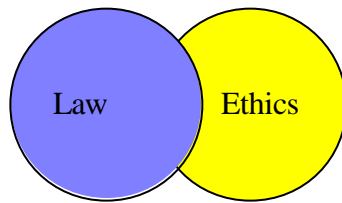


Illustration 1. Moderate Overlap

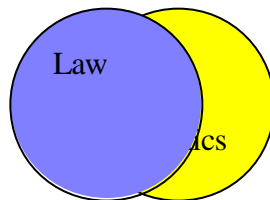


Illustration 2. Considerable Overlap

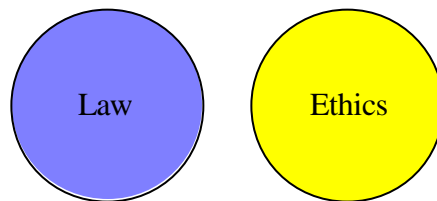


Illustration 3. No Overlap

Evaluating CNA capabilities against the body of international law that governs war should be coupled with an evaluation against an ethical framework. The ethical

⁵ Personal Interview with Dr. Albert C. Pierce (Annapolis, MD: U.S. Naval Academy, Nov 2000).

framework that has heavily influenced international law concerning war, the Just War Tradition, may prove useful in ethical consideration of CNA. An examination of CNA, international law governing war, and the Just War Theory is necessary to determine the validity of this claim. Finally, conclusion and recommendations on this matter are offered.

Chapter 2

CNA and DOD Posture

Policy Guidance

The goal of offensive IO is to "affect adversary's decision makers and or achieve or promote specific objectives."⁶ While this goal is necessarily broad to encompass a full range of capabilities and situations, it is by no means unrestricted. According to the DOD public affairs guidance and Joint Pub 3-13, the use of CNA as a form of offensive IO must embrace the following principles:

a. Objectives must be clearly established and support overall national and military objectives, and must include identifiable indicators of success.

b. Selection and employment of capabilities must be appropriate to the situation, consistent with U.S. objectives and must be consistent with the Law of Armed Conflict, domestic and international law and applicable rules of engagement (ROE).

c. Consequences of employing specific capabilities must be predictable with a predetermined level of confidence.

⁶ Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations* (Ft Monroe, VA: Joint Warfighting Center, 1998), II-1.

d. Planning may involve non-DOD forces, agencies, or organizations and must be thoroughly integrated, coordinated, and de-conflicted with all other elements (land, sea, air and space) of an operation or campaign.

e. Approval of the use of CNA by the National Command Authorities (NCA) is required.

The above principles, to a certain degree, embrace both legal and ethical considerations, and support a reasonable expectation that USCINCSpace will develop more concrete policies concerning the use of CNA.

Planning

According to guidance in Joint Pub 3-13, USCINCSpace will rely on the Joint Operation Planning and Execution System (JOPES) to guarantee at least a detailed and systematic approach to CNA planning.⁷ This is particularly true of peacetime or deliberate planning, a two-year cycle, which permits full employment of the JOPES process and participation of the Joint Planning and Execution Community (JPEC). Time sensitive or crisis action planning will follow an abbreviated JOPES process and, as such, will not be as detailed as a deliberate plan. CNA planning

⁷ Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations* (Ft Monroe, VA: Joint Warfighting Center, 1998), V-I.

expertise does not exist at the theater unified command level or joint task force level, however, the Unified Commander's Information Operations Planning Cell and other organizations (i.e., Joint Information Operations Center and Land Information Warfare Activity) support planning.⁸ IO are incorporated in the target review process, and are heavily influenced by intelligence support, ROE, and legal review.

The use of CNA, in the context of the principles set forth, the planning oversight offered by JOPES and the involvement of the NCA may serve to mitigate unintended consequences of this new capability. In the past, militaries have deployed new technologies and techniques without careful consideration of their broader implications. The U.S. use of nuclear weapons on Japan, and Germany's decision to target Great Britain's populace are two such examples from World War II.

CNA and Potential Targets

As a form of offensive IO, CNA is an operation designed to disrupt, deny, degrade, or destroy information resident on computers and computer networks or the

computers and networks themselves.⁹ CNA can be used directly to disrupt or destroy an adversary's information infrastructure or it can be a technique to facilitate other functional methods of offensive IO. These methods include, but are not limited to, operations security (OPSEC), military deception, psychological operations, electronic warfare (EW), physical attack/destruction, and special information operations (SIO).

CNA and the other methods of offensive IO represent the incorporation of information technology into longstanding military practices. Martin Libicki, a recognized expert in the field of Information Warfare and former Senior Fellow of the National Defense University, states:

Certain aspects of IW are as old as history; striking at the enemy's head, deception of all sorts and psychological operations in general...EW reached prominence in World War II. The more recent automation of command center has created more vulnerable targets reachable via iron bombs, and against penetrable systems through malevolent software. If societies evolve in the virtual dimension, the significance and frequency of hacker war and cyberwar would be greatly increased. Psychological operations would also be greatly transformed.¹⁰

⁸ James M. McCarl, LTCOL, USA, *Planning Offensive Information Operations* (Quantico, VA: Marine Corps War College, Marine Corps University, 1999), 18.

⁹ Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations* (Ft Monroe, VA: Joint Warfighting Center, 1998), I-9.

¹⁰ Martin C. Libicki, *What is Information Warfare* (Washington, DC: National Defense University, 1997) http://www.ndu.edu/irmc/publications/educ_the_dod.htm.

Consistent with current military targeting, some examples of IO targets, extracted from Joint Pub 3-13 are shown in Illustration 4. CNA, like conventional weapons can destroy both military and civil targets. "Unlike most kinetic weapons, however, it can reach across the world at the speed of light passing over many international borders en route to its target...cyber weapons can target large masses of people in both military and civilian communities."¹¹ The unique nature of the capability will demand well-considered policy on its use and the class of targets.



Figure I-8. Examples of Information Operations Targets

¹¹ William J. Bayles, LTCOL, USA, *Moral and Ethical Considerations for Computer Network Attack As A Means of National Power in Time of War* (Washington, DC: National Defense University Press, 2000), 19.

Illustration 4. Examples of Information Operations
Targets¹²

Methods of CNA

The methods of CNA include, but are not limited to: physical destruction, offensive software, "sniffing" or wiretapping of networks, tempest-style eavesdropping of electronic devices, "chipping" or hardware based malicious software embedded surreptitiously in systems, directed energy weapons, and dissemination of misinformation.¹³ These methods can be used singly or in combination to accomplish a wide range of strategic, operational and tactical goals. The United States' air strike on the command and control system of Iraqi anti-air weapons in January 2001 is an example of physical destruction of an information system in support of an operational goal.

Offensive software, which includes "viruses" like "worms", "Trojan Horses" and other forms of malicious code (defined in Glossary under computer virus), offers many options. General Richard Myers, USCINCSpace, provides an example of the tactical use of offensive software, "the degrading of an air defense network of an adversary through

¹² Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations* (Ft Monroe, VA: Joint Warfighting Center, 1998), I-17.

¹³ Campen, Dearth & Gooden, ed. *Cyberwar: Security, Strategy and Conflict In the Information Age* (Fairfax, VA: AFCEA International Press, 1996), 245.

manipulating ones and zeros as opposed to dropping 2,000 pound bombs on radars.”¹⁴ On a larger magnitude, offensive software attacks on an enemy’s critical systems (stock or commodity exchanges, electric power grids, ground and air traffic control systems, health care systems) could wreak havoc on a country’s economy and cause major societal disruption, physical damage, and substantial loss of life.

“Sniffing” and tempest-style eavesdropping on electronic devices of an adversary’s information system can gain critical information about the adversary. For example, information gained from an adversary’s logistic support system, using this method of CNA, may provide insight into an adversary’s course of action before and during a conflict.

“Chipping” or software surreptitiously embedded in hardware systems offers a distinct advantage. For instance, the U.S. was accused of altering AT&T telephone switching equipment exported to Poland in the early 1970’s to allow the U.S. to remotely shut down the communications infrastructure in the event of an attack. ¹⁵

Directed-energy weapons, such as electromagnetic pulse (EMP) guns and bombs, and High Energy Radio Frequency

¹⁴ Richard Myers, GEN, USAF, *CINCUSPACECOM, DOD News Briefing on Jan 5, 2000*, <http://www.infowar.com/MIL-C4I>.

(HERF) guns, debilitate or destroy the electronics of computers, communications, satellites or power systems. This capability can be employed to achieve an infoblockade by disabling a critical node, which could result in little or no electronic information entering or leaving a nation's borders.¹⁶

Dissemination of information through CNA can support the full range of PSYOP and deception activities. An enemy's radio and television network could be taken over electronically and then used to broadcast propaganda in support of a political objective.¹⁷ Specifically, video and audio morphing of a political leader may serve to affect the will of the people.

The above examples of employing CNA are consistent with existing military practice but present extraordinary legal and ethical challenges, in that the magnitude of the effects of CNA raises concerns of discrimination, proportionality, and military necessity. Discrimination, the principle that recognizes the difference in treatment between combatants and noncombatants, can easily be compromised with CNA. For instance, an offensive software

¹⁵ Campen, Dearth & Gooden, ed, *Cyberwar: Security, Strategy and Conflict In the Information Age* (Fairfax, VA: AFCEA International Press, 1996), 246.

¹⁶ Sean P. Kanuck, *Recent Development, Information Warfare: New Challenges for Public International Law*, (Harvard International: 37 L.J. 272, 289, 1996).

¹⁷ Peter Grier, *Information Warfare*, Air Force Magazine (March 1995).

strike against a critical node of the air defense network could inadvertently affect the adversary's critical non-military systems.

Proportionality means the amount of good accomplished by an attack is greater than harm done. Degrading an adversary's logistic support information system could also compromise the integrity of the adversary's military medical databases thus hampering its ability to treat the wounded. In this case, the act can be considered disproportionate to the desired results.

Military necessity, which allows latitude for those actions not specifically forbidden, is still restrictive. An infoblockade could be an effective method in getting the enemy to capitulate; however, the effects of an infoblockade may violate proportionality and noncombatant immunity. For example, such an attack against a country heavily vested in globalization could have a detrimental impact on the country's economy and livelihood of its citizens.

With CNA, as with other weapons and capabilities, commanders are bound to the discriminate and proportionate use of force to accomplish its objectives. An assessment of these criteria with CNA may require more scrutiny than conventional capabilities. With conventional weapons the

effects are generally known and or relatively easier to assess. The same is not necessarily true for CNA.

Chapter 3

CNA and International Law

To corroborate the need for a broader base for ethical considerations for CNA, the legal review process and its associated problems are examined. This examination will include some of the international laws that may apply to CNA and examples of anomalies in applying these laws to CNA.

DOD Instruction 5000.2, Defense Acquisition, dated 23 Oct 00, mandates General Counsel (GC) and Judge Advocate General (JAG) review of intended acquisitions of potential weapons to determine if they are consistent with U.S. obligations. This instruction also encourages legal review of "new, advanced or emerging technologies, which may lead to development of weapons and weapons system."¹⁸ The DOD analytical framework for evaluating new weapons and capabilities involves a three-part test:

- a. Does the weapon cause unnecessary suffering?
- b. Is the weapon discriminating?

¹⁸ Department of Defense Instruction, 5000.2, *Defense Acquisition* (Washington, DC: Department of Defense, 23 Oct 00).

c. Does the weapon or capability violate specific treaty law?

The validity of the test rests in the fact that it incorporates the laws and customary practices that govern war. The first two parts of the three-part test serve to focus the lawyer's attention on international laws formulated at the 1907 Hague Convention and the 1949 Geneva Conventions.

Based on the premise that the rights of belligerents to adopt means of injuring the enemy are not unlimited, the 1907 Hague Convention forbade the employment of arms, projectiles or materials calculated to cause unnecessary suffering. The Hague Convention also set forth guidance on the matter of military necessity and neutrality. In the matter of military necessity, Hague authorizes the use of measures not specifically forbidden by international law, which are indispensable for securing the submission of the enemy.¹⁹ In reference to neutrality, the territory and rights of neutral states are inviolable by the forces of belligerents.²⁰

The four 1949 Geneva Conventions addressed in detail the protection of wounded combatants, certain medical and

¹⁹ Hague Convention (IV) Respecting the Laws and Customs of War on Land (1907).

²⁰ Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and persons in Case of War on Land (1907).

religious persons, hospitals and medical transportation, and every civilian. The underlying theme of the statutes of the Geneva Conventions is the distinction principle, which states:

Parties shall at all times distinguish between the civilian population and combatants and shall direct their operations only against military objectives; parties are obliged, to the extent possible, to remove civilians and civilian objects from the vicinity of military objectives. In choosing means and methods of attack regard must be paid to minimize incidental loss, injury and damage to civilian and civilian objects. No attack should be launched in which the anticipated civilian losses would be excessive in relation to the concrete and direct military advantage anticipated.²¹

The legal review of interpreting these laws with respect to developing and deploying CNA will require intense scrutiny. Practices that may have been legal with conventional capabilities may stretch the limits on legality when applied to CNA. For example, infoblockades can be tantamount to economic sanctions that are often the first choice among U.S. strategies. Such sanctions are usually aimed at the political leadership, as was the case with the insurgent leadership in Haiti in 1991; however, the unintended consequence was that the people bore the brunt of the pain and suffering. With an infoblockade, the probability and magnitude of suffering by the people could

²¹ Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War (1949).

be unacceptably high, if the country as a whole is very dependent on information systems. Even relatively straightforward issues like neutrality, pose a dilemma in an information warfare environment:

An attack through a network that crosses neutral territory or using a neutral country's satellites, computers or networks would infringe upon that neutral's territory, just as would an overflight by a squadron of bombers or an incursion of troops. The attack could be considered illegal and perhaps, an act of war against the neutral... Although this argument is strong a counter argument exists. The encroachments beyond a nation's borders that may violate its neutrality have in the past been physical intrusions by troops, ships or planes. Attacking a neutral's networks satellites, or computers might not violate the states neutrality because it might not involve physical encroachment.²²

The last part of the three-part test would look to law specifically addressing CNA. At present no such specific international law exists. CNA, however, may be subject to principles of several laws, including those that prohibit certain forms of deception (i.e., perfidy), interference of a nation's broadcast (International Telecommunication Convention), or the use of space to deploy certain weapons (the Outer Space Treaty).²³

While the three-part legal review test is a valuable tool, there are no specific guidelines as to the approach to be taken in this review. One lawyer's approach may be

to determine ways and circumstances that a new capability may be used, while another lawyer's approach may be to determine ways and circumstances a capability cannot be used. A third lawyer may approach the review from both directions. The lawyer's approach, experience and knowledge of the technology factor into the quality of the legal review process.

The indirect nature of CNA and its potential to impact large numbers of people can compromise noncombatant immunity, challenge acceptable paradigms concerning military necessity and unnecessary suffering, and bring new dimensions to discussions on proportionality. Understandably, international law offers no specific restrictions on CNA, in that the development of international law generally lags behind the development of technology. Where international law does not exist, the burden of proper restrictions of CNA rests on the policymakers and developers, and on their legal support team. The bottom-line is that total reliance on the legal review process limits the ethical considerations for the use of CNA.

²² Greenberg, Goodman, Soo Hoo, *Information Warfare and International Law* (Washington, DC: DOD Command and Control Research Program, Jan 1998), 27-28.

²³ International Telecommunication Convention.

Chapter 4

Just War Theory and CNA

The Just War Theory, which is the foundation for much of the international law governing war, may offer conceptual guidance concerning the legal and ethical use of CNA. The purposes of this discussion are to outline the principles of the Just War Theory and apply these principles to a notional scenario.

Just War Theory is divided into two categories, the morality for war (jus ad bellum) and the morality in war (jus in bello). Jus ad bellum has to do with when it is just to resort to military force while jus in bello deals with what is justified in the use of force. In order to justify an act of war, all the principles in jus ad bellum and jus in bello must be satisfied. These principles, whose early expressions came from theologians, have been elaborated and expanded upon by many scholars. James Turner Johnson, an expert in the area of Just War, presents a version of the theory as seen in Table 1.

Table 1. The Just War Tradition as a Source of Criteria for Ethical Judgment²⁴

| Criteria | Definition |
|--|---|
| <i>Jus ad Bellum</i> (the right to resort to force) | |
| Right Authority | The person or body authorizing the use of force must be the duly authorized representative of a sovereign political entity. The authority to use force implies the ability to control and cease that use: that is a well-constituted and efficient chain of command. Classic Statement: Reservation of the right to employ force to persons or communities with no political superior. |
| Just Cause | The protection and preservation of value. Classic Statement: Defense of the innocent against attack; retaking person, property or other values wrongly taken; punishment of evil. |
| Right Intention | The intent must be in accord with the just cause and not territorial aggrandizement, intimidation, or coercion. Classic Statement: Evils to be avoided in war, including hatred of the enemy, “implacable animosity,” “lust for vengeance” desire to dominate. |
| Last Resort | Determination at the time of the decision to employ force that no other means will achieve the justified ends sought. Interacts with other jus ad bellum criteria to determine level, type and duration of force employed. |
| Proportionality of Ends | The overall good achieved by the force use of force must be greater than the harm done. The levels and means of using force must be appropriate to just ends sought. |
| Reasonable Hope | Prudential calculation of the likelihood that the means used will bring the justified ends sought. Interacts with other jus ad bellum criteria to determine level, type, and duration of force employed. |
| The Aim of Peace | Establishment of international stability, security, and peaceful interactions. May include nation building, disarmament, other measures to promote peace. |
| <i>Jus in Bello</i> (the employment of force) | |
| Noncombatant Protection/Immunity (Discrimination) | Definition of noncombatancy; avoidance of direct, intentional harm to noncombatants; efforts to protect them. Classic Statement: List of classes of person (clergy, merchants, peasants on the land, other people) in activities not related to the prosecution of war to be spared the harm of war. |

²⁴ James Turner Johnson, *Morality and Contemporary Warfare* (New Haven and London: Yale University Press, 1999), 28-29.

| | |
|--------------------------|---|
| Proportionality of Means | Means causing gratuitous or otherwise unnecessary harm are to be avoided. Prohibition of torture. Classic statement: Attempts to limit weapons, days of fighting, person who should fight. |
|--------------------------|---|

This theory offers a base for a systematic approach to ethical considerations of CNA that can be put to use immediately. Consider the following scenario. For the past five years, relationships between the U.S. and Country X have been tenuous for a variety of reasons. Country X took credit for a recent denial of service attack of a U.S. government computer network causing a significant loss in man-hours and productivity. U.S. intelligence sources have not confirmed if Country X is indeed responsible for this attack.

Refugees from Country X bring to the attention of the international community the violations of human rights in Country X. The U.S. seeks diplomatic engagement with Country X on these human rights issues. Resenting the U.S. involvement in its national affairs, Country X boasts of a CNA capability that can disrupt the U.S. financial systems (Wall Street), and threatens to do so in a matter of days.

The U.S. agrees to postpone discussions on the human rights issues, partly to avoid aggression and partly due to

the ambivalence of its allies. Country X, nonetheless, continues in its threat against U.S. financial systems.

The U.S. has the CNA capability to defend against this threat by a precision attack on the command and control system of Country X's military headquarters. This command and control system is a part of Country X's national information infrastructure, which is the backbone of all of its nation's critical information systems to include other military, government and financial systems. In an effort to sway Country X away from aggression, the U.S. purposely leaks information to Country X about this CNA capability, but to no avail.

Based on failures in diplomacy and the urgency for a response to the threat, the U.S. deems a military response as inevitable. Deliberations on the type of force and when this force can be employed bring to the forefront the CNA capability. Although there is only a remote possibility that the CNA will damage Country X's critical national infrastructure, a thorough ethical review is necessary.

Applying the Just War Theory to this scenario aids and expands the legal review process by providing a framework to gather and analyze information. This analysis will address each of the Just War criteria and then provide an

assessment as to the morality of an attack on Country X's military headquarters command and control system.

Right Authority

As outlined in policy, approval of a CNA rests with the NCA. In addition, such an attack qualifies as an act of war, which would require the involvement of Congress. As well as having a well-defined chain of command to meet the right authority criterion, the NCA must also be able to control the CNA. In the scenario, the level of precision and the possible results of the CNA response are acceptable. This information is critical to support the justified use of CNA. The ideal level of precision would be a controllable soft-kill of the command and control systems.

Just Cause

The protection of U.S. financial information assets calls for some type of action. Whether the CNA is justified depends largely on the credibility of the threat. Country X's claim that it compromised U.S. systems in the past is not validated. The U.S. is not reasonably sure that Country X can do what it is now threatening to do.

All information systems are vulnerable to attack, but efforts in information assurance have served to minimize vulnerabilities. This brings into question the issue of how well the U.S. financial systems can sustain such an attack. It is reasonable to assume that Wall Street systems are protected by anti-intrusive software and frequent back-ups are common practice. The fact that the threat by Country X is not entirely creditable and the U.S. could sustain this attack with manageable loss does not substantiate a just cause determination.

Right Intentions

The situation as delineated in the scenario supports a justifiable intent for the use of the subject CNA, in that, the sole purpose for considering this CNA is protection from Country X's threat. In addition, this show of force may serve to deter Country X from further aggression against the U.S. Even if further aggression were imminent, the distraction to Country X as a result of the attack would be advantageous to the U.S. in preparing for follow-on actions.

By pondering intentions, decision-makers can address beforehand possible misconceptions. For instance, if

Country X is an economic competitor of the U.S., the CNA could be misconstrued as a demonstration of the power the U.S. has to effect Country X's critical information systems. To secure the support of the American people, possible misconceptions like the one stated above must be addressed.

Last Resort

U.S. attempts to leverage its political power against Country X have failed. Economic and informational elements of national power wielded against Country X will not produce the immediate results that are necessary to eliminate the threat. The scenario, right or wrong, implies that the U.S. has met the criterion of last resort. Validating the CNA as a viable military option must be satisfied. Discussions on all the possible options and consequences must ensue. With or without knowledge of the other military options, the CNA response would be difficult to justify. For the same reason the CNA failed to meet the just cause criterion, it will also fail as an act of last resort. The passive measures in place to protect the financial information system make validating this attack as a last resort unfounded. Another reason the CNA would fail

as an act of last resort is also linked to the following discussion on the matter of reasonable hope.

Reasonable Hope

The reasonable hope that the CNA would be successful in protecting the U.S. financial system against the threat is very high. Implied in the scenario, the success of this CNA hinges on striking first for optimum results. Striking first when danger is imminent is justified. According to Michael Walzer, a recognized expert on morality in war, both individuals and states can rightfully defend themselves against violence that is imminent but not actual and can fire the first shots if they know themselves about to be attacked. "Even the most presumptuous aggressor is not likely to insist, as a matter of right, that his victim stands still until he lands the first blow."²⁵

In the scenario, Country X's threat is borderline credible and its capability to act on the threat is relatively unknown. A first strike by the U.S. in the form of the proposed CNA would be more a response to prevent aggression than a response to an imminent attack. Walzer strongly warns against preventive strike when immediate security is not at risk:

...the hostility is prospective and imaginary, and it will always be a charge against us that we have made war upon soldiers who were themselves engaged in entirely legitimate (non-threatening) activities. Hence the moral necessity of rejecting any attack that is merely preventive in character, that does not wait upon and respond to the willful acts of an adversary.²⁶

The CNA attack would probably meet the criterion of reasonable hope, if U.S. and Country X were already engaged in armed conflict, but not as a first strike for the purpose of prevention.

Proportionality of Ends

The CNA meet the criterion of proportionality of ends. An attack on the command and control information system of the military headquarters is appropriate to the ends sought - the protection of U.S. financial information systems. The good gained from protecting the financial data of innocent Americans outweighs the disruption of the command and control systems of Country X's headquarters.

The Aim of Peace

A focus on the aim of peace seeks an assessment of the rationale of the CNA in enhancing the security of the U.S. and aids in stabilizing relationships between the U.S. and

²⁵ Michael Walzer, *Just and Unjust War*, 3rd Ed. (New York, NY: Basic Books, 1977), 74.

Country X. Nothing in the scenario suggests that the U.S. is not driven by the aim of peace. Whether or not the CNA will bring peace is elusive. Absent an assessment of Country X's resolve, its overall military readiness and the will of its people, it is naïve to assume aggression by Country X would end by eliminating its capability to impact U.S. financial systems. This CNA could very well play to Country X's desires to escalate violence. On the other hand, not using this CNA could serve to postpone peace by making the U.S. vulnerable to further harassment by Country X and other countries, as it deals with a potential financial crisis. Regardless of the dichotomy presented above, it is still reasonable to justify the aim of peace. The use of this CNA during armed conflict increases the U.S. ability to provide the overwhelming force necessary to get Country X to capitulate and sue for peace.

Noncombatant Protection

While the potential to compromise noncombatant immunity with an indiscriminate CNA attack is high, this is not the case with the proposed attack. The command and control system of the military headquarters of Country X as a target poses no direct threat to noncombatants. The

²⁶ Michael Walzer, *Just and Unjust War*, 3rd Ed. (New York, NY: Basic Books, 1977), 80.

precision of this CNA eliminates the concern over unintended consequences and as such presents the ideal standard for all CNA.

Proportionality of Means

Consideration on proportionality of means deals with the potential to cause gratuitous or unnecessary harm. One would be hard pressed to make an argument that the proposed CNA has the potential to do unnecessary harm. A kinetic response is obviously premature, but a non-kinetic response like this CNA would be appropriate to protect U.S. financial information assets. Also, the fact that information systems can be restored or replaced supports the proportionality of this CNA.

Overall Assessment

The proposed CNA failed several criteria of the Just War Theory and as such is not justified. The purpose of this scenario, however, is not to merely present a set of circumstances where a CNA is justified or not justified, but to validate a process for ethical analysis of the use of CNA. In reality, the issues and circumstances surrounding the use of a CNA could be so convoluted that

making an assessment on its justified use can be far more difficult than the decision derived from the scenario. The Just War Theory offers a framework to support such difficult determinations.

Even when it is obvious that a criterion in the Just War Theory is not met, continuing in the process of ethical considerations provide insight as to when such an attack would be justified. As mentioned earlier, modification of the CNA to affect a controllable soft kill of the command and control system is ideal. Also gleaned from the analysis is that one of the reasons that the act was not justified is purely a function of time. Striking first is not an option, but the capability can be used during armed conflict to eliminate a continuing threat against U.S. financial systems. The Just War Theory as a framework for ethical consideration of CNA provides familiar ground for discussion and also serves to provide insight in setting standards for use of CNA.

Chapter 5

Conclusion and Recommendations

Development of policy on the use of CNA is in its infancy. DOD recognizes the advantages of this capability as well as its legal ramifications. International law will to some degree serve to guide decision-makers on the ethical use of this weapon, but is limited as a framework for a full discussion of the ethical use of CNA.

The goals of CNA are consistent with current military practice but their impact can be far reaching. The dual use (military and civilian) of information systems, the possibility of inadvertent, unnecessary suffering of civilians, and the potential for intentional and unintentional misuse, dictate a clearly defined approach for ethical considerations. The Just War Theory can serve as a foundation for such an approach.

Advocating the adequacy of the Just War Theory as a framework for moral consideration in modern warfare, James Turner Johnson summarizes that the Just War Theory: corresponds to the moral values of our culture, provides a conceptual framework for moral analysis and judgment, and

produces practical moral guidance as well as identifies the relevant moral values for the situation at hand.²⁷

Applying the Just War Theory, in itself, poses some difficulties. Michael Walzer offers an expansion of the Just War tradition in what he calls "practical morality." War, he writes, is a social phenomenon and as such is subject to social revision, which makes applying a theoretical framework difficult.²⁸ Walzer seeks to defend the business of arguing in moral terms, saying that the framework is less important than the process. To support his argument, he focuses on the difficulty in assessing the criteria within the Just War Theory that make its use problematic. In reference to the difficulty in judging right intentions, Walzer believes contrary to many others that the developers of the atomic bomb were driven by a deep moral anxiety, specifically,

...they (the scientists) sought it (the assignment) out, taking the initiative, urging upon President Roosevelt the critical importance of an American effort to match the work being done in Nazi Germany...because of acute sense of what a Nazi victory would mean for their native lands and all mankind.²⁹

For Walzer, the value of any system of morals is to present a common moral language for debate on real life

²⁷ James Turner Johnson, *Can Modern War Be Just?* (New Haven and London : Yale University Press, 1984), 17.

²⁸ Michael Walzer, *Just and Unjust War*, 3rd Ed. (New York, NY: Basic Books, 1977), 14.

²⁹ Ibid, 263.

application. He offers what he calls the war convention, which is the "set of articulated norms, customs, professional code, legal precepts, religious and philosophical principles and reciprocal arrangement that shape military conduct."³⁰

Although Johnson advocates the Just War Theory and Walzer advocates a common language and utilitarian approach to morality in war, a synthesis of the two views provides some guidelines for moral consideration of CNA:

a. Military planners should ensure that their decisions are not devoid of a thorough ethical review;

b. Just War Theory is still a viable framework in that it provides a common language for discussion of CNA and serves to highlight the moral importance of consequences.

c. The application of any system of morals is difficult and imperfect, but must be practical in that it allows room for social revisions and the situation at hand.

Employing the Just War Theory as a framework provides a systematic approach and common language and is flexible enough to address a variety of concerns. Weight can be assigned to criteria and new criteria can be added. In addition, the process of applying these principles can

³⁰ Ibid, 44.

serve as a foundation for the development of future laws and customary practice. This is not to say that sound ethical decisions cannot be made without it, but this approach can serve as a useful tool for lawyers, policymakers and developers to use in organizing and evaluating their decisions.

The ethical dilemma posed by CNA is expected to be the subject of many writings. Some of the early writings serve to highlight the concerns and others suggest the need of new methodology for evaluating the ethical use of CNA. This paper supports the Just War Theory as a base for ethical considerations that can be tailored to address the issues associated with CNA.

Glossary

chipping. Hardware based malicious software embedded surreptitiously in systems.

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA.

computer virus. Typically a short program designed to disperse copies of itself to other computers and disrupt those computers' normal operations. A computer virus usually attaches or inserts itself to or in an executable file or the boot sector (the area that contains the first instructions executed by a computer when it is started or restarted) of a disk; those that infect both files and boot records are called bimodal viruses. A distinction should be made between a virus-which must attach itself of another program to be transmitted-and a bomb, a worm, and a Trojan horse. A **bomb** is a program that resides silently in a computer's memory until it is triggered by a specific condition, such as a date. A **worm** is a destructive program that propagates itself over a network, reproducing as it goes. A **Trojan horse** is a malicious program that passes itself off as a benign application; it cannot reproduce itself and, like a virus, must be distributed by diskette or electronic mail.

defense information infrastructure. The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information System Network and includes command and control, tactical, intelligence, and commercial communication systems to transmit DOD information. Also called DII.

electromagnetic pulse. A pulse of electromagnetic energy, capable of disrupting computers, computer networks, and

many forms of telecommunication equipment. Also called EMP.

electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW.

global information infrastructure. The worldwide interconnection of communication networks, computer databases, and consumer electronics that make vast amounts of information available to users. Also called GII.

high energy radio frequency weapon. A device that can disrupt the normal operation of digital equipment such as computers and navigational equipment by directing HERF emissions at them. Also called HERF weapon.

infoblockade. An offensive information operation that results in the permitting little or no electronic information to enter or leave a nation's borders.

information assurance. Information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.

information operations. Actions taken to affect adversary information systems while defending one's own information and information systems. Also called IO.

information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW.

logic bomb. Unauthorized computer code, sometimes delivered by email, which, when executed, checks for particular conditions or particular states of the system which, when satisfied, triggers the perpetration of an unauthorized, usually destructive.

morphing. Manipulation of electronic data with the intent to deceive.

national information infrastructure. The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. Also called NII.

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision-makers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack.

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC.

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP.

sniffing. The making of a secret to computer networks to record information sent over them.

special information operations. Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. Also called SIO.

TEMPEST. Military code-name for activities related to monitoring the activity of a computer or other electronic equipment by detecting low levels of electromagnetic emissions from the device, and technology to defend against such monitoring.

vulnerability. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system.

BIBLIOGRAPHY

- Alberts, David S., *The Unintended Consequences of Information Age Technologies*. Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1996.
- Aldrich, Richard W., *Cyberterrorism and Computer Crimes: Issues Surrounding The Establishment of an International Regime, INSS Occasional Paper 32, Information Warfare Series*. USAF Academy, CO: USAF Institute for National Security Studies, 2000.
- Aldrich, Richard W., *The International Legal Implications of Information Warfare, INSS Occasional Paper 9, Information Warfare Series*. USAF Academy, CO: USAF Institute for National Security Studies, 1996.
- Armed Forces Staff College (AFSC) Pub 12, *Joint Information Warfare Staff Officer's Guide*. Norfolk, VA: Armed forces Staff College, 1998.
- Bayles, William J. LTCOL, USA, *Moral and Ethical Considerations for Computer Network Attack As A Means of National Power in Time of War*. Washington, DC: National Defense University Press, 2000.
- Campen, Dearth & Gooden, ed. *Cyberwar: Security, Strategy and Conflict In the Information Age*. Fairfax, VA: AFCEA International Press, 1996.
- Chairman, Joint Chiefs of Staff, *Joint Vision 2020*. Washington, DC: U.S. Government Printing Office, June 2000.
- Department Of Defense Instruction, 5500.15, *Defense Acquisition*. Washington, DC: Department of Defense, October 2000.
- Greenberg, Lawrence, Goodman, Seymour, SooHoo, Kevin, *Information Warfare and International Law*. Washington DC: Institute for National Strategic Studies, National Defense University, 1997.
- Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War (1949).
- Grier, Peter, *Information Warfare*, Air Force Magazine (March 1995).
- Hague Convention (IV) Respecting the Laws and Customs of War on Land (1907).
- Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (1907).

- Johnson, James Turner, *Can Modern War Be Just?* New Haven and London: Yale University Press, 1999.
- Johnson, James Turner, *Morality and Contemporary Warfare*. New Haven and London: Yale University Press 1999.
- Joint Chiefs of Staff, Joint Pub 3-13, *Joint Doctrine for Information Operations*. Ft Monroe, VA: Joint Warfighting Center, July 1998.
- Law of War Detachment Marine Corp University, Brief on Law of War. New Orleans, LA: 2000.
- Libicki, Martin C., *What is Information Warfare*. Washington DC: National Defense University, 1997, http://www.ndu.edu/irmc/publications/educ_the_dod.htm.
- Kanuck, Sean P., *Recent Development, Information Warfare: New Challenges for Public International Law*. Harvard International: 37 L.J.272,289, 1996.
- McCarl, James M., LCOL, USA, *Planning Offensive Information Operations*. Quantico, VA: Marine Corps War College, Marine Corps University, May 1999.
- Mosley, Alex, *Just War Theory*. Internet Encyclopedia of Philosophy, 1998 <http://www.utm.edu/research/iep/j/justwar.htm>.
- Myers, Richard, GEN, USAF, *CINCUSPACECOM, DOD News Briefing on Jan 5, 2000*, <http://www.infowar.com/MIL-C4I>.
- Nagle, William, ed. *Morality and Modern Warfare*. Baltimore, MD: Helicon Press, 1960.
- Neilson, Robert e., *Sun Tzu and Information Warfare*. Washington, DC: National Defense University Press, 1997.
- Nitzberg, Sam, "Conflict and the Computer: Information Warfare and Related Ethical Issues", <http://www.iamsam.com>, 2000.
- Pierce, A. "Just War Principles and Economic Sanctions", Ethics and International Affairs, 1996.
- Personal Interview with Dr. Albert C. Pierce, Annapolis, MD: U.S. Naval Academy, Nov 2000.
- SECDEF WASHINGTON DC//OASD-PA/DPL// Public Affairs Guidance – Computer Network Attack, DTG 012050Z Nov 00.
- Walzer, Michael, *Just and Unjust War*, 3rd Ed. New York, NY: Basic Books, 1977.